**BÁO CÁO BÀI THỰC HÀNH: DENIAL OF SERVICE (DoS) ATTACKS**

**I. Mục Tiêu**

Bài thực hành nhằm giúp sinh viên hiểu rõ nguyên lý hoạt động của các kiểu tấn công DoS, cách thức triển khai và tác động của chúng đối với hệ thống mục tiêu. Các hình thức tấn công được thực hiện trong bài gồm:

- SYN Flood Attack: Tấn công bằng cách gửi hàng loạt gói SYN nhằm làm cạn kiệt tài nguyên kết nối TCP của mục tiêu.

- ICMP Flood Attack: Tấn công bằng cách gửi lượng lớn gói ICMP để làm nghẽn băng thông mạng của mục tiêu.

- Ping of Death Attack: Tấn công bằng cách gửi các gói ping quá lớn, vượt quá kích thước cho phép, nhằm gây lỗi hệ thống.

Thông qua thực hành, sinh viên sẽ hiểu rõ cách phòng chống và bảo vệ hệ thống trước các kiểu tấn công này.

**II. Môi Trường Thực Hành**

***1. Thiết Bị Sử Dụng***

- Máy tấn công: Kali Linux (PLABKALI01)

+ Địa chỉ IP: 172.22.78.110

+ Công cụ: hping3, Metasploit Framework, ping

- Máy mục tiêu: Windows Server (PLABWIN10)

+ Địa chỉ IP: 172.22.64.141

+ Công cụ: Wireshark, Task Manager

***2. Các Bước Chuẩn Bị***

- Kiểm tra kết nối mạng giữa hai máy bằng lệnh ping.

- Tắt Windows Firewall trên Windows Server để đảm bảo tấn công không bị chặn.

- Mở Wireshark trên Windows Server để theo dõi lưu lượng mạng.

**III. Nội Dung Thực Hành**

***1. Task 1 - SYN Flooding Attack***

- Mục tiêu: Gửi liên tục các gói SYN nhằm làm quá tải bảng kết nối trên Windows Server.

- Công cụ: **hping3**

- Thực hiện:

***hping3 -S 172.22.64.141 -a 172.22.78.110 -p 80 --flood***

- Quan sát:

+ Wireshark ghi nhận lượng lớn gói SYN gửi đến Windows Server.

+ CPU của Windows Server tăng đột biến.

+ Windows Server bị chậm, mất kết nối tạm thời.

- Kết quả: Tấn công gây ảnh hưởng rõ rệt đến hiệu suất hệ thống.

***2. Task 2 - ICMP Flood Attack***

- Mục tiêu: Tấn công bằng cách gửi số lượng lớn gói ICMP để tiêu tốn tài nguyên băng thông mạng.

- Công cụ: **hping3**

- Thực hiện:

***hping3 -c 10000 --icmp 172.22.64.141***

- Quan sát:

+ Wireshark ghi nhận hàng ngàn gói ICMP gửi đến mục tiêu.

+ Windows Server phản hồi chậm do quá tải xử lý gói tin.

- Kết quả: Tấn công làm tăng tải mạng nhưng không làm sập hệ thống do tài nguyên chưa bị cạn kiệt.

***3. Task 3 - Ping of Death Attack***

- Mục tiêu: Gửi các gói ping có kích thước lớn hơn giới hạn cho phép nhằm gây lỗi hệ thống.

- Công cụ: ping

- Thực hiện:

***ping -s 65500 172.22.64.141 -t***

- Quan sát:

+ Task Manager ghi nhận mức sử dụng tài nguyên mạng tăng cao.

+ Windows Server có dấu hiệu chậm lại, nhưng không bị crash.

- Kết quả: Hệ thống bị ảnh hưởng nhẹ, nhưng không bị sập hoàn toàn.

***4. Task 4 - SYN Flood Attack Using Metasploit***

- Mục tiêu: Sử dụng Metasploit để thực hiện SYN Flood chuyên sâu.

- Thực hiện:

***use auxiliary/dos/tcp/synflood***

***set RHOST 172.22.64.141***

***set RPORT 80***

***set SHOST 172.22.78.110***

***set TIMEOUT 50000***

***exploit***

- Quan sát:

+ Task Manager trên Windows Server ghi nhận mức sử dụng CPU cao.

+ Hệ thống phản hồi chậm hơn so với SYN Flood bằng hping3.

- Kết quả: Tấn công đạt hiệu quả cao hơn do Metasploit tối ưu hóa gửi gói tin.

**IV. Kết Quả và Nhận Xét**

***1. Kết Quả***

- SYN Flood Attack gây ảnh hưởng mạnh nhất, khiến hệ thống chậm đáng kể.

- ICMP Flood Attack tiêu tốn tài nguyên mạng nhưng không làm sập hệ thống.

- Ping of Death Attack làm chậm máy chủ nhưng không gây gián đoạn nghiêm trọng.

- Sử dụng Metasploit cho kết quả mạnh hơn nhờ tối ưu hóa gói tin tấn công.

***2. Nhận Xét***

- DoS là dạng tấn công nguy hiểm có thể gây gián đoạn dịch vụ nếu không có biện pháp phòng chống.

- Một hệ thống có firewall và giới hạn băng thông tốt có thể giảm thiểu ảnh hưởng của DoS.

- Các phương pháp tấn công trong lab chưa đạt mức DDoS vì chỉ có một nguồn tấn công.

- Để đánh giá DoS toàn diện, có thể thử nghiệm trên các hệ thống thực tế với nhiều nguồn tấn công hơn.

**V. Các Biện Pháp Phòng Chống DoS/DDoS**

- Sử dụng Firewall và IDS/IPS để phát hiện và ngăn chặn các gói tin đáng ngờ.

- Giới hạn băng thông cho các dịch vụ quan trọng để tránh bị tấn công quá tải.

- Sử dụng các dịch vụ CDN và Load Balancer để phân tán lưu lượng truy cập.

- Cấu hình hệ thống bảo vệ TCP/IP, chẳng hạn như giảm thời gian chờ của kết nối TCP.

- Giám sát mạng liên tục để phát hiện sớm các dấu hiệu tấn công.

**VI. Kết Luận**

- Bài thực hành giúp sinh viên hiểu rõ cơ chế tấn công DoS và cách thức bảo vệ hệ thống.

- Các tấn công này có thể được sử dụng để kiểm tra độ bền vững của hệ thống mạng.

- Các biện pháp phòng chống DoS là cần thiết để bảo vệ hệ thống trước các mối đe dọa mạng.

**VI. Tài Liệu Tham Khảo**

1. Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd Edition, Wiley, 2020.
2. William Stallings, *Cryptography and Network Security: Principles and Practice*, 7th Edition, Pearson, 2017.
3. RFC 4987 - *TCP SYN Flooding Attacks and Common Mitigations*, Internet Engineering Task Force (IETF).
4. Trang chủ Kali Linux: <https://www.kali.org/>
5. Tài liệu Metasploit Framework: https://docs.metasploit.com/

**Lưu ý**: Báo cáo này được thực hiện trong môi trường kiểm soát và hợp pháp. Bạn không nên thử nghiệm trên mạng không dây mà bạn không có quyền truy cập.